

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography offenses committed by **GEORGE M. GIBBS III**. This Affidavit is submitted in support of Applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following:
  - a. The residential property located at **2803 STONE MILL PLACE, BEAVERCREEK, OHIO, 45434** (hereinafter referred to as the “**SUBJECT PREMISES**” and more fully described in Attachment A-1 hereto); and
  - b. The person of **GEORGE M. GIBBS III** (hereinafter referred to as “**GIBBS**” and more fully described in Attachment A-2 hereto).
3. This Affidavit is submitted in support of Applications for search warrants for the **SUBJECT PREMISES**, the person of **GIBBS**, and the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **GIBBS**. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:
  - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2), which make it a crime to possess child pornography; and
  - b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.
4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the **SUBJECT PREMISES**, the person of **GIBBS**, and the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **GIBBS**. It does not contain every fact known to the investigation.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1), are present at the **SUBJECT PREMISES**, on the person of **GIBBS**, and on the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **GIBBS**.

#### **PERTINENT FEDERAL CRIMINAL STATUTES**

8. 18 U.S.C. §§ 2252(a)(2) and (b)(1) state that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
9. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) state that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
10. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or

facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

### **BACKGROUND INFORMATION**

#### **Definitions**

12. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:
  - a. “**Child Pornography**” includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
  - b. “**Visual depictions**” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
  - c. “**Minor**” means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
  - d. “**Sexually explicit conduct**” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

- e. **“Child erotica”**, as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- f. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- g. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- h. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- i. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

- j. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- k. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.
- l. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### Background on Computers and Child Pornography

- 13. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- 14. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the



photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

15. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
16. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.
17. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
18. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

19. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### Collectors of Child Pornography

20. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
  - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
  - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
  - d. Collectors may possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often

discard child pornography images only while “culling” their collections to improve their overall quality.

- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

#### Kik Messenger Application

- 21. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
- 22. The Kik messenger application is administered by MediaLab.ai Inc., a company based in Santa Monica, California. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
- 23. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. MediaLab.ai Inc. does not verify this information, and as such, users can provide inaccurate information.
- 24. MediaLab.ai Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, MediaLab.ai Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. MediaLab.ai Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). MediaLab.ai Inc. does not store or maintain chat message content.



25. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

#### Virtual Private Networks

26. A Virtual Private Network, commonly known as a VPN, provides programming that creates a safe and encrypted connection over a less secure network, such as the public Internet. A VPN works by using a shared public infrastructure while maintaining privacy through security procedures and tunneling protocols.
27. A VPN extends a private network across a public network, and it enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device (such as a laptop, desktop computer, or smartphone) across a VPN may benefit from the functionality, security, and management of the private network. Encryption is a common though not inherent part of a VPN connection. A number of Electronic Service Providers offer VPN's to customers worldwide.
28. VPN's assign users different IP addresses and run users' data through different servers. As a result, it is very difficult (if not often virtually impossible) for third parties to track the users' identities and browsing activities. Based on my training and experience, I know that individuals involved in child pornography offenses and other illegal activities sometimes use VPN's to conceal their activities from law enforcement officers.

#### Cloud Storage

29. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing is the delivery of computing services – including servers, storage, databases, networking, software, analytics, and intelligence – over the Internet (the “cloud”). Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations.
30. Mega is a cloud storage and file hosting service offered by Mega Limited (Ltd.), an Auckland, New Zealand-based company. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.
31. Mega provide its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a “sharing link”. A sharing link creates a URL to store

the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

#### NCMEC and CyberTipline Reports

32. The National Center for Missing and Exploited Children (commonly known as “NCMEC”) was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
33. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the CyberTipline reports. These ICAC’s review the CyberTipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

#### FACTS SUPPORTING PROBABLE CAUSE

##### Records from MediaLab.ai Inc.

34. On or around December 4, 2020, MediaLab.ai Inc. filed a report to NCMEC’s CyberTipline regarding suspected child pornography and/or child exploitation files that were located in a Kik account utilizing the user name of kuro\_shinigami444. NCMEC forwarded MediaLab.ai Inc.’s CyberTipline report, along with the suspected child pornography or child exploitation files, to the FBI for further investigation. I obtained and reviewed the CyberTipline Report and the accompanying files as part of the investigation.
35. On or around January 12, 2021, MediaLab.ai Inc. was served with an administrative subpoena requesting subscriber information for the kuro\_shinigami444 Kik account as well as the log of IP addresses that were utilized to access the account. On or around July 28, 2021, MediaLab.ai Inc. was served with a federal search warrant requesting information associated with the kuro\_shinigami444 Kik account. Although MediaLab.ai Inc. does not maintain the contents of messages for its account users, it does maintain various log files regarding the activity occurring in the accounts – such as transactional chat logs (which are logs of all messages that users have sent and received) and chat platform logs (which are logs of media files that users have sent and received).

36. Below is a summary of some of the information contained in the CyberTipline report and the records received from MediaLab.ai Inc. in response to the subpoena and search warrant:
- a. The kuro\_shinigami444 Kik account was created on or around June 19, 2019. The profile name for the account was "Showgolden".
  - b. The email address of karate\_niidan06@yahoo.com was associated with the account profile. The records identified that this email address had been confirmed or verified by a representative of MediaLab.ai Inc.
  - c. The account was last accessed on or around December 23, 2020.
  - d. The Kik account was installed onto a Samsung Android device bearing Model SM-A515U1 on or around September 8, 2020.
  - e. Approximately nine videos depicting suspected child pornography and/or child exploitation material were located in the kuro\_shinigami444 Kik account and reported to NCMEC in the CyberTipline report. The report identified that approximately six of the videos were shared in a messaging group(s) by the kuro\_shinigami444 account user, and that approximately three of the videos were sent by the kuro\_shinigami444 account user to one (or more) other user(s) via private chat message(s). The report indicated that MediaLab.ai Inc. discovered the approximately nine video files in the kuro\_shinigami444 Kik account on or around December 3, 2020.
  - f. I have reviewed the approximately nine video files that MediaLab.ai Inc. discovered in the kuro\_shinigami444 Kik account. Based on my review of the files and my training and experience, I believe that at least approximately six of the videos depict child pornography. I further believe that the remaining approximately three videos depict possible child pornography (i.e., files depicting possible children, although I could not conclude with sufficient certainty if the individuals were in fact minors). By way of example, two of the files depicting child pornography are described as follows:
    - i. 6bd8eaa1-7dee-44b7-96f0-405e02cf016d.mp4: The file is a video that depicts what appears to be a nude toddler-aged female child on a bed. What appears to be a white male (whose face is not captured in the video) fondles the toddler's vagina with his hand, masturbates his penis, and rubs his penis on the toddler's vagina. The toddler also touches the male's penis with her hand. The video is approximately one minute and 59 seconds in duration. The log files identified that the kuro\_shinigami444 Kik account user distributed this video file to another user via a private chat message on or around November 27, 2020.

- ii. 2d732b33-56d1-4fcc-a9d8-08010ebf9711.mp4: The file is a video that depicts what appears to be a nude pre-pubescent white female child and a nude pre-pubescent white male child. The female child performs fellatio on the male child's penis and fondles his penis with her hand. The video is approximately one minute and 58 seconds in duration. The log files identified that the kuru\_shinigami444 Kik account user distributed this video file to approximately 25 other users via a group chat message on or around November 25, 2020.
- g. The log of IP addresses for the account indicated that a number of IP addresses serviced by Verizon and Servers Australia Pty. Ltd. were utilized to access the account.
  - i. Based on Internet research, it appears that Servers Australia Pty. Ltd. is a VPN provider based in Australia. Their website indicates that the company hosts other VPN providers throughout the world.
  - ii. Based on my training and experience, I know that the use of IP addresses serviced by Servers Australia Pty. Ltd. is consistent with someone using a VPN to access the Internet. I also know that the use of IP addresses serviced by Verizon is consistent with someone using the data plan from his/her cellular telephone or tablet to access the Internet.
  - iii. Again based on my training and experience, I know that individuals who utilize VPN's on their computer devices do not always take the time or effort needed to log into the VPN's when accessing the Internet. It is not uncommon for such individuals to sometimes utilize the Internet service from the data plans on their cellular telephones or tablets and/or from the wireless Internet service at their residences.

Records from Oath Holdings Inc.

37. On or around January 12, 2021 and July 14, 2021, Oath Holdings Inc. (the service provider for Yahoo email accounts) was served with administrative subpoenas requesting subscriber information for the karate\_niidan06@yahoo.com email account as well as the log of IP addresses that were utilized to access the account. On or around July 28, 2021, a federal search warrant was served to Oath Holdings Inc. requesting information associated with the karate\_niidan06@yahoo.com account (to include the contents of the email account). Records received from Oath Holdings Inc. in response to the two administrative subpoenas and the federal search warrant included the following information:
- a. The karate\_niidan06@yahoo.com account was created on or around December 12, 2006.

- b. The user name for the account was “**GEORGE GIBBS**”. The user’s birthday was listed as being XX/XX/1988 (redacted for purposes of this Affidavit).
  - i. This birthday matches **GIBBS**’ date of birth.
- c. The telephone number of 937-475-2654 was associated with the account. The records identified that this telephone number had been verified by a representative of Oath Holdings Inc.
- d. The account was last accessed on or around July 28, 2021 (the date of the issuance of the search warrant).
- e. The log of IP addresses identified that the following IP addresses were utilized to access the account:
  - i. IP addresses serviced by Servers Australia Pty. Ltd. and several other providers that also appear to be associated with VPN’s;
  - ii. IP addresses serviced by the Verizon cellular telephone network; and
  - iii. An IP address serviced by AT&T (that being 99.88.157.4).
- f. More than 850 email messages were contained in the account. A number of these messages included information indicative that **GIBBS** is the user of the account. By way of example, some of these messages included the following:
  - i. At least approximately 15 of the sent email messages contained “**GEORGE GIBBS III**”, “**GEORGE M. GIBBS III**”, or “**G. GIBBS III**” in the signature line.
  - ii. In or around March 2020, the karate\_niidan06@yahoo.com account user exchanged email messages with an individual who appeared (based on the signature line) to be the Director of Human Resources and Risk Management for a company based in California. In the messages, the karate\_niidan06@yahoo.com account user requested copies of his prior W2 tax forms. As part of making the request, the karate\_niidan06@yahoo.com account user identified that his name was “**GEORGE M. GIBBS III**”, his date of birth was XX/XX/1988 (redacted for purposes of this Affidavit), the last four digits of his social security number were 5717, and that he resided at 2803 Stone Mille Place in Beavercreek, Ohio.
    - 1. The date of birth and last four digits of the social security number that were provided by the karate\_niidan06@yahoo.com account user in



the email message matches **GIBBS'** date of birth and social security number. As detailed below, **GIBBS** uses the **SUBJECT PREMISES** on his current Ohio driver's license.

- g. On or around December 23, 2020, the karate\_niidan06@yahoo.com account user received an email message from an email address associated with the CyberGhost VPN provider. The email provided a license key needed to activate a CyberGhost VPN account.
  - i. As noted above, IP addresses associated with several VPN's were utilized to access the karate\_niidan06@yahoo.com email account and the kuru\_shinigami444 Kik account.
- h. On or around February 20, 2021, approximately four email messages were received by the karate\_niidan06@yahoo.com account from an email address associated with the Mega cloud storage provider. The email messages indicated that a Mega account associated with the karate\_niidan06@yahoo.com email address had been created on or around February 20, 2021.
- i. On or around July 17, 2021, an email message was sent from karate\_niidan06@yahoo.com to karate\_niidan06@yahoo.com. The only text in the body of the message was a URL that appeared to be associated with a sharing link to a Mega account.
  - i. Based on my training and experience, I know that individuals sometimes email files and/or URL's to themselves for a variety of reasons, including but not limited to the following: (1) to store the files and/or URL's in a secure location that is outside of their computer devices, (2) to provide a means to access the files and/or URL's on different devices, or (3) in preparation to email the files and/or URL's to others.
  - ii. As detailed above in the background section of the Affidavit, I know that individuals commonly utilize cloud storage accounts such as Mega to store their files. Also as detailed above, I know that it common for individuals to trade child pornography files by sending sharing links to cloud storage accounts.

#### Other Subpoenaed Records

- 38. Verizon was identified as being the service provider for telephone number 937-475-2654. On or around February 4, 2021, Verizon was served with an administrative subpoena requesting subscriber information for this telephone number. Records received from Verizon in response to the subpoena included the following information:

- a. The telephone number was subscribed to “**GEORGE GIBBS III**” at the **SUBJECT PREMISES**.
  - b. The account was activated on or around July 3, 2020, and it was active as of the date of the subpoena.
  - c. The device that utilized the telephone number was a Samsung A51 bearing Model SM-A515U1-VS.
    - i. As noted above, the kuro\_shinigami444 Kik account was installed on a device bearing the same model on or around September 8, 2020.
39. On or around July 14, 2021 and August 9, 2021, AT&T was served with two administrative subpoenas requesting subscriber information for the IP address of 99.88.157.4 on a sample of four of the dates and times that it was utilized to access the karate\_niidan06@yahoo.com email account (four dates during the approximate time period of August 12, 2020 to include July 28, 2021). Records received in response to the subpoena identified that this IP address was subscribed to “**GEORGE GIBBS**”<sup>1</sup> at the **SUBJECT PREMISES**. The records further identified that the Internet account was active as of on or around August 2, 2021.
40. On or around August 7, 2021, Mega Ltd. was served with an administrative subpoena requesting subscriber information for any Mega accounts associated with the email address karate\_niidan06@yahoo.com as well as the log of IP addresses that were utilized to access the account. Records provided by Mega Ltd. in response to the subpoena included the following information:
- a. Consistent with the emails located in the karate\_niidan06@yahoo.com email account, a Mega account associated with this email address was created on or around February 20, 2021. The user name for the account was “**GEORGE GIBBS**”.
  - b. Two IP addresses were utilized to access the account: 98.88.157.4 (the IP address that is subscribed to “**GEORGE GIBBS**” at the **SUBJECT PREMISES**) and an IP address that appears to be associated with a VPN.
41. As detailed above, on or around July 17, 2021, the karate\_niidan06@yahoo.com account user emailed himself what appeared to be a Mega sharing link. On or around August 7, 2021, Mega Ltd. was served with an administrative subpoena requesting subscriber information for the Mega account that had posted this sharing link, as well as the log of IP addresses that were utilized to access the account. Based on the records provided by Mega Ltd. in response to the subpoena, it did not appear that **GIBBS** was the user of this account – specifically, the account was associated with an email address and IP addresses that do not appear at this time to be associated with **GIBBS**. It is therefore reasonable to believe that

---

<sup>1</sup> As detailed in the subsequent paragraph, it appears **GIBBS**’s father’s name is also George Gibbs. It is unknown if **GIBBS** or his father is the subscriber of the Internet account.

**GIBBS** had received this sharing link from another individual.

Mega Sharing Link

42. On or around August 5, 2021, I typed the URL to the above noted Mega sharing link (the URL located in the karate\_niidan06@yahoo.com email account) into an Internet browser and was routed to a publicly accessible portion of a Mega account. The sharing link contained a total of approximately 505 video files that were saved in approximately nine file folders. No encryption key or password was required to access the video files. The videos primarily depicted pre-pubescent children, teenagers, and young adults engaged in sexually explicit conduct. Based on my review of the files and my training and experience, I believe that at least approximately 267 of the videos depict child pornography. A number of the other videos depict possible child pornography (i.e., files depicting possible children, although I could not conclude with sufficient certainty if the individuals were in fact minors). By way of example, two of the files depicting child pornography are described as follows:
- a. (pthc) NEW 2016 Pedo Childlover 8yo Daddy's Little Girl JM 10.mp4: The file is a video that depicts what appears to be a nude pre-pubescent white female child lying on her back with her legs spread apart. What appears to be an adult white male performs cunnilingus on the child. The child sits up, and the adult male inserts his penis into the child's mouth. The adult male proceeds to masturbate his penis and secrete semen onto the child's vagina. The video is approximately 10 minutes and 43 seconds in duration. The video was saved in a file folder entitled "Eating pussy".
  - b. VID-20201008-WA0053.mp4: The file is a video that depicts what appears to be a pre-pubescent white female child who is wearing a shirt and a skirt pulled up around her waist but no underwear. The child is lying on her back with her legs spread apart. What appears to be an adult white male engages in vaginal sexual intercourse with the child. The video is approximately 18 seconds in duration. The video was saved in a folder entitled "Cumshot".

Search Warrant at the **SUBJECT PREMISES**

43. On or around August 23, 2021, search warrants were authorized by the United States District Court for the Southern District of Ohio for the **SUBJECT PREMISES** and **GIBBS'** person. Agents and officers of the FBI and the Beavercreek Police Department executed the warrants on or around August 27, 2021. **GIBBS**, Adult A (**GIBBS'** father), Adult C (**GIBBS'** wife), and a juvenile child were present when agents and officers arrived to execute the warrants. Among other items, the following were seized pursuant to the warrants:
- a. A Samsung A51 Model SM-A515U1 cellular telephone, which was seized from **GIBBS'** bedroom;

- i. As noted above, the kuro\_shinigami444 Kik account was installed on a device bearing the same model on or around September 8, 2020.
  - b. An Acer laptop, which was seized from **GIBBS'** bedroom;
  - c. A black Western Digital external hard drive, which was seized from a backpack in **GIBBS'** bedroom;
  - d. A black and orange PHD 3.0 Silicon-Power portable hard drive, which was seized from a backpack in **GIBBS'** bedroom; and
  - e. Two iPhones, which Adult A (**GIBBS'** father) identified as belonging to him.
- 44. During the execution of the search warrants, **GIBBS** agreed to be interviewed after being advised of his Miranda rights. Below is a summary of some of the information provided by **GIBBS** during the interview:
  - a. **GIBBS** resided at the **SUBJECT PREMISES** with his wife (Adult C); his parents (Adult A and Adult B); and his and Adult C's two juvenile children.
  - b. **GIBBS** had a Samsung cellular telephone bearing telephone number 937-475-2654. The telephone was in his bedroom.
  - c. **GIBBS** had a laptop computer that was in his bedroom as well a black external hard drive and an orange external hard drive. **GIBBS** was shown the black Western Digital external hard drive and the black and orange PHD 3.0 Silicon-Power portable hard drive that were recovered from the backpack in his bedroom, and he confirmed that these devices belonged to him.
  - d. **GIBBS** utilized the email address karate\_niidan06@yahooo.com (the email address associated with the kuru\_shinigami444 Kik account).
  - e. **GIBBS** began viewing pornography as a child, and he developed a significant addiction to pornography.
  - f. **GIBBS** began viewing child pornography in mid- or late-2020 after another individual sent him a child pornography file via the Wickr messenger application. He thereafter developed an addiction to child pornography.
  - g. **GIBBS** traded child pornography files with others via the Wickr and Kik messenger applications. His Wickr account name was "showgolden", and his Kik account name was kuru\_shinigami444. **GIBBS** also obtained and viewed child pornography files

from the TOR<sup>2</sup> website. He obtained and viewed both images and videos of child pornography depicting children of all ages. **GIBBS** occasionally utilized the child pornography files to masturbate.

- h. **GIBBS** utilized his Samsung cellular telephone to access his Wickr and Kik accounts. He did not save the child pornography files onto his cellular telephone but rather saved the files to his black external hard drive. He transferred the files from his cellular telephone to his external hard drive by connecting both devices to his laptop.
- i. There were times when **GIBBS**' trading partners sent him child pornography files via sharing links to Mega accounts. **GIBBS** opened a Mega account utilizing the karate\_niidan06@yahoo.com email address so that he could better access these links. **GIBBS** denied saving any child pornography files to his Mega account.
- j. **GIBBS** sometimes emailed himself the Mega sharing links containing child pornography that he received from others so that he could access the links at later times. **GIBBS** recalled emailing Mega links to himself in 2020, but he did not recall emailing himself any links in July 2021.
- k. **GIBBS** was "banned" from Kik in December 2020 because child pornography files were found in his account. He attempted to stop viewing child pornography at that time, and he deleted the child pornography files from the black external hard drive. **GIBBS** later "relapsed" and continued trading child pornography with others on Wickr. He also utilized a computer software program to recover some (but not all) of the child pornography files he had deleted from the black external hard drive.
- l. **GIBBS** last traded child pornography files with others via Wickr a few weeks ago. **GIBBS** noted that messages and files contained in the Wickr application were automatically deleted from his account after the passage of time based on the security settings, so the child pornography files he obtained a few weeks ago may no longer be in his Wickr account.
- m. **GIBBS** previously operated and was an instructor at a martial arts studio called Japan Karate-do. He closed the studio in 2020 because of the Coronavirus pandemic.

#### Examination of Computer Devices

45. Pursuant to the search warrant, the Samsung A51 Model SM-A515U1 cellular telephone that

---

<sup>2</sup> The Onion Router (TOR) is a free and open-source software that provides users with anonymous communications and browsing on the Internet. The software directs Internet traffic through a free, worldwide volunteer overlay network consisting of more than seven thousand relays. This network conceals a user's location and usage from anyone conducting network surveillance or traffic analysis.



was seized from the **SUBJECT PREMISES** (which **GIBBS** identified as being the device he utilized to access his Kik and Wickr accounts and to trade child pornography files) was examined. Below is a summary of some of the information recovered during the examination:

- a. The telephone number for the device was 937-475-2654 (the number that **GIBBS** identified as being his telephone number).
  - b. The karate\_niidan06@yahoo.com email account was established on the telephone.
  - c. The Wickr application was installed on the telephone. An account with a user name of "showgolden" was logged into on the application. No messages were saved in the account that contained child pornography files. However, it was noted that the showgolden account user had contacts saved in the account for other users with the following account names: "childporn", "youngporn", "loli"<sup>3</sup>, "kiddyporn", and "loligirl". On or around August 23, 2021, the showgolden account user sent messages to the "childporn", "youngporn", and "loli" account users inquiring about whether or not their accounts were still active.
  - d. Consistent with the information provided by **GIBBS**, no child pornography files were recovered from the device during the preliminary examination.
  - e. At least approximately four documents were saved on the telephone that contained **GIBBS'** name on them.
46. Also pursuant to the search warrant, the black Western Digital external hard drive (which was the device that **GIBBS** identified that he used to save his child pornography files) was examined. Below is a summary of some of the information recovered during the examination:
- a. Recovered from the device were approximately 396 images and approximately 635 videos depicting child pornography. Many of the child pornography files were saved in various sub-folders contained within a folder entitled "Black", a subfolder entitled "The Stash", another subfolder entitled "Extras", and another subfolder entitled "Child Porn". By way of example, two of the files depicting child pornography are described as follows:
    - i. Playing with Toddler Daughter.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child. The child is first

---

<sup>3</sup> "Lolita", sometimes shortened to "loli", is often used as a term to refer to prepubescent or adolescent female children who are attractive and sexually promiscuous. The term originated from a novel about an affair between a man and his 12-year old stepdaughter. Based on my training and experience, I know that "Lolita" and "loli" are search terms that individuals sometimes utilize to search for child pornography files.

depicted standing nude in a room. The child is then depicted in a bathtub with what appears to be a nude adult white male. The child touches the adult male's penis and performs fellatio on the adult male. The child also stands up at one point, and the camera zooms in on her vagina and buttocks. The child and adult male are then depicted in another setting. The child again performs fellatio on the adult male. The adult male masturbates his penis and secretes semen onto the child's vagina and abdomen. The video ends by displaying the following text: "Aint I good to you lol.....". The video is approximately three minutes and 36 seconds in duration.

- ii. Daddy Touched Daughter During Diaper Change.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child. Another individual removes the child's diaper and digitally penetrates her vagina. The video is approximately one minute and 27 seconds in duration.

- b. Saved on the device were approximately 495 of the 505 files that I observed in and downloaded from the Mega sharing link noted above (the link contained in the email message sent to and from the karate\_niidan06@yahoo.com account on or around July 17, 2021). The files were saved in the same nine folders as those contained in the Mega sharing link. The metadata for the files identified that the files from approximately four of the folders were saved onto the external hard drive on or around July 17, 2021, and that files from approximately five of the folders were saved onto the external hard drive on or around July 19, 2021.

- c. A number of images and videos depicting **GIBBS** were saved on the device.

47. Also pursuant to the search warrant, the black and orange PHD 3.0 Silicon-Power portable hard drive (which **GIBBS** identified as belonging to him) was examined. Below is a summary of some of the information recovered during the examination:

- a. Recovered from the deleted space of the device were approximately 9,519 images and approximately 820 videos depicting child pornography. By way of example, two of the files depicting child pornography are described as follows:
  - i. File with hash value of 6e3536f5d266c21ef89afc6517ce4830c0beb16e: The file is an image that depicts what appears to be a white toddler-aged female child who is wearing a dress but no pants or underwear. The child has a pacifier in her mouth. The child is lying on her back with her legs straddled, and what appears to be an adult white male's penis is inserted into her anus.
  - ii. File with hash value of 33937da4ebe825b1b1f589cfd38d8e78255d7902: The file is an image that depicts what appears to be a nude pre-pubescent white female child. The child is hung upside down from a rope, and a bandana is covering her eyes. An object is inserted into the child's vagina.

- b. A number of images and videos depicting **GIBBS** were saved on the device.
48. Again pursuant to the search warrant, the Acer laptop (the device that **GIBBS** identified that he used to transfer his child pornography files from his cellular telephone to his external hard drive) was examined. Below is a summary of some of the information recovered during the examination:
- a. Various artifacts were recovered during the examination that were indicative that **GIBBS** was the user of the laptop. For example, images and videos depicting **GIBBS**, a resume with **GIBBS**' name on it, and an application for a Social Security Card with **GIBBS**' name on it were saved on the laptop. Also by way of example, over one thousand four hundred artifacts were recovered from the laptop that included the email address karate\_niidan06@yahoo.com.
  - b. At least approximately 864 images depicting child pornography were recovered from the laptop. The child pornography files were recovered from a file path that stores thumbnail images for files that have been viewed on the laptop and from the deleted space of the laptop. By way of example, two of the files depicting child pornography are described as follows:
    - i. File with a hash value of 50b29fc56b0fd517319496aad7542e862a65301a:  
The file is an image that depicts what appears to be a nude pre-pubescent white female child kneeling on what appears to be a bed. What appears to be an adult white female is spreading apart the child's buttocks and licking (or close to licking) the child's anus.
    - ii. File with a hash value of e6af169607df33b285833ab4132cb11c1b410a27:  
The file is an image that depicts what appears to be a nude pre-pubescent white female child lying on what appears to be a board or table. The child is bound to the board or table with a white rope. What appears to be a nude adult white male is standing over the child, and his penis is in the child's mouth.
  - c. Various artifacts were recovered from the computer that included file names and file folder names matching those from the Mega sharing link noted above (the link contained in the email message sent to and from the karate\_niidan06@yahoo.com account on or around July 17, 2021). Although the files themselves were not saved on the laptop, the artifacts were indicative that a number of those files and file folders had been accessed and/or viewed on the laptop during the approximate time period of July 17, 2021 through July 19, 2021 (which is consistent with the dates that the files were saved onto the Western Digital external hard drive). Some of the artifacts were also indicative that at least some of the files from the Mega sharing link were previously saved on the desktop of the laptop in a folder entitled

“DESTROY ASAP” and a subfolder entitled “Hetero”.

- d. A cellular telephone with a name of “George’s Galaxy A51” (consistent with **GIBBS’** Samsung cellular telephone) and a Western Digital external hard drive with a serial number matching that of the device seized from the backpack in **GIBBS’** bedroom had both been attached to the laptop as recently as on or around August 10, 2021.
    - i. This information is consistent with **GIBBS** utilizing his laptop to transfer his child pornography files from his Samsung cellular telephone to his Western Digital external hard drive.
49. The two iPhones that **GIBBS’** father identified as belonging to him were examined. No child pornography files were recovered from these two devices.

Arrest and Conviction of **GIBBS**

50. Based on the information detailed above, there is probable cause to believe that **GIBBS** was the user of the following in 2021:
- a. The kuru\_shinigami444 Kik account;
  - b. The showgolden Wickr account;
  - c. The Samsung A51 Model SM-A515U1 cellular telephone bearing telephone number 937-475-2654 that was recovered from **GIBBS’** bedroom at the **SUBJECT PREMISES**;
  - d. The black Western Digital external hard drive and PHD 3.0 Silicon-Power portable hard drive that were recovered from **GIBBS’** bedroom at the **SUBJECT PREMISES**; and
  - e. The Acer laptop that was recovered from **GIBBS’** bedroom at the **SUBJECT PREMISES**.
51. There is also probable cause to believe that **GIBBS** committed the following violations in 2021:
- a. **GIBBS** utilized his Samsung cellular telephone and his Kik and Wickr accounts to distribute child pornography.
  - b. **GIBBS** received and downloaded child pornography files from Mega sharing links.

- c. **GIBBS** utilized his Western Digital external hard drive, PHD 3.0 Silicon-Power portable hard drive, and Acer laptop to possess and access with the intent to view child pornography files.
52. On or around September 14, 2021, Magistrate Judge Sharon L. Ovington signed a Criminal Complaint and arrest warrant charging **GIBBS** with two counts of distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); two counts of receipt of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).
  53. On or around September 15, 2021, **GIBBS** came to the FBI's office in Centerville, Ohio at my request. Upon his arrival, **GIBBS** was taken into custody pursuant to the arrest warrant. Several items of personal property were collected from **GIBBS'** person, including a Samsung cellular telephone bearing model SM-S111DL<sup>4</sup> and an IMEI number of 352319150023008. Pursuant to **GIBBS'** consent, these items were released to his father later that day.
  54. On or around September 20, 2021, a detention hearing was held for **GIBBS** before Magistrate Judge Ovington. Magistrate Judge Ovington ordered **GIBBS** to be released pursuant to home detention and electronic monitoring pending the resolution of the criminal case. As part of the terms of his release, **GIBBS** was forbidden from accessing any computer devices capable of accessing the Internet and any sexually explicit materials. **GIBBS** was released from custody on or around September 24, 2021.
  55. On or around September 28, 2021, an indictment was returned in the United States District Court for the Southern District of Ohio charging **GIBBS** with three counts of distribution of child pornography, in violation of 18 U.S.C. §2252(a)(2) and (b)(1); one count of receipt of child pornography, in violation of 18 U.S.C. §2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2). On or around March 14, 2022, **GIBBS** pled guilty to one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2).
  56. I have spoken to the officer from the United States Pretrial Services Office who currently supervises **GIBBS**. This officer informed me of the following information:
    - a. **GIBBS** has resided at the **SUBJECT PREMISES** from the time that he was released from custody in September 2021 through the present. Pretrial Services

---

<sup>4</sup> The model number that was documented by the officer who completed the property receipt was SM-111DL. From Internet research, I know that there is a Samsung cellular telephone bearing model number SM-S111DL, but that there are no Samsung cellular telephones with a model number of SM-111DL (i.e., without the "S" in front of the 111DL). Internet research of the IMEI number for the cellular telephone identified that the telephone was a Samsung device bearing model SM-S111DL. Therefore, it appears that the officer committed a transcriptionist error when writing down the model number.



officers have conducted periodic home visits and have confirmed that **GIBBS** resides at the **SUBJECT PREMISES**.

- b. **GIBBS** and his father are the only individuals who currently reside at the **SUBJECT PREMISES**. **GIBBS**' mother, wife, and children have all moved out of the residence.
- c. **GIBBS** has not received authorization to utilize any electronic devices. He is supposed to use the home's landline telephone when making any telephone calls.

Post-Arrest Activity on Kik Messenger

- 57. Throughout 2022, agents and investigators of the Salt Lake City, Utah division of the FBI have conducted online investigations to identify individuals utilizing social media and messenger applications to commit child exploitation offenses. As part of these investigations, an FBI online covert employee (hereinafter referred to as "OCE") routinely accessed group chats that promoted the distribution and receipt of child pornography.
- 58. On or around March 12, 2022, OCE was invited into a group chat on the Kik messenger application by another group member. This group had a user name of "#underfifteen" and a profile name of "You nnow". OCE briefly participated in this group chat and exchanged private messages with two of the group's administrators. OCE observed child pornography files being distributed in the group. Below is a summary of OCE's communications and observations while he was in the group and communicated with the administrators:
  - a. Upon entering the group, OCE observed a standard message that detailed the rules of the group. These rules identified that in order to be accepted into the group, users must do the following: (1) identify their "ASL" (a term to refer to age, sex, and location) upon two minutes of entering the group, and (2) send one of the group's administrators a "PM" (a term to refer to a private message) with two pictures or one video depicting "young" content. Various other rules were detailed, including a rule that the "oldest talkers" were at risk of being removed from the group.
    - i. Based on my training and experience, I know that administrators of groups that trade child pornography on messenger applications such as Kik often require that users send child pornography files in order to be accepted into the groups. The administrators also often remove members who are not actively sharing child pornography files. These practices are enforced as a means to prevent law enforcement officers from entering and/or remaining in the groups and to ensure that everyone is contributing to the supply of child pornography files.

- b. Four administrators were identified for the group, including one with a user name of Sentai\_Sensei<sup>5</sup> and a profile name of “GEO The Banhammer”<sup>6</sup> and another with a user name thebestone1985 and a profile name of “Naughty Screwdriver”. The above detailed message identified that if none of the administrators were available to verify a new user, the user should send his/her files to the Sentai\_Sensei user. OCE observed that the profile picture for the Sentai\_Sensei account user was a picture of a person wearing a black hood and a mask. The background picture for the Sentai\_Sensei account user was a picture of the torso and legs of a white male who was wearing only underwear and was lying on a bed.
  - i. Administrators of Kik groups have the ability to create groups, invite or remove members, and create rules for the group. However, a current administrator may or may not be the person who created the group.
- c. OCE observed that approximately 100 Kik users were in the #underfifteen group.
- d. After entering the #underfifteen group, OCE initially purported himself to be a 16-year old female. OCE asked who he should private message to provide his verification files. The Kik user with the user name of thebestone1985 and a profile name of “Naughty Screwdriver” instructed OCE to message him.
- e. OCE sent a private message to the thebestone1985 account user and sent this user a picture that OCE purported to be of himself (posing as the 16-year old child). The thebestone1985 account user responded that this picture was not what OCE was supposed to send and instructed OCE to contact “geo” (referring to the Sentai\_Sensei Kik account user with the profile name of “GEO The Banhammer”).
- f. OCE sent a private message to the Sentai\_Sensei Kik account user. OCE and the Sentai\_Sensei account user had the following discussion:
  - i. The Sentai\_Sensei account user said that the way that OCE had entered the Kik group was a violation of the group’s rules.
  - ii. OCE sent the Sentai\_Sensei account user a picture of a purported female child. The Sentai\_Sensei account user told OCE that verification files for the group typically involved pictures or videos of “young content, meaning CP”. The Sentai\_Sensei account user further advised that the group only accepted things like “young nudes or something close to it”.

---

<sup>5</sup> Sensei is a term to refer to a teacher or instructor, usually of a Japanese martial arts studio. As noted above, GIBBS previously was an instructor at a martial arts studio.

<sup>6</sup> Banhammer is a term to refer to the power of moderators and system administrators to ban users from digital space.

1. “CP” is a common term to refer to child pornography.
- iii. OCE told the Sentai\_Sensei account user that he was not actually a 16-year old female child but rather was a 38-year old male who had a 16 year old daughter. OCE commented that he was looking to trade files with other parents.
- iv. The Sentai\_Sensei account user told OCE that the group was intended for sharing files, not trading files. The Sentai\_Sensei account user also said that because OCE was untruthful about his “ASL” (age, sex, and location), OCE had violated the group’s rules. The Sentai\_Sensei account user told OCE that he needed to leave the group.
- g. While in the #underfifteen group chat, OCE observed the thebestone1985 account user posted three video files into the group chat. Based on my training and experience, I believe that at least two of the videos depict child pornography. I further believe that the third video depicts possible child pornography (i.e., a file depicting a possible child, although I could not conclude with sufficient certainty if the individual was in fact a minor). The two files depicting suspected child pornography are described as follows:
  - i. RYMG8216.mp4: The file is a video that depicts what appears to be a nude adult white male having vaginal sexual intercourse with what appears to be a nude white or Hispanic female child. The video is approximately 21 seconds in duration.
  - ii. JQHC9716.mp4: The file is a video that depicts what appears to be a nude white male and a pre-pubescent white female child who is wearing clothing. The two individuals are sitting next to each other. The white male reaches into the child’s shorts, and it appears that he fondles her vagina. The female child also uses her hand to masturbate the male’s penis. The video is approximately two minutes in duration.
- h. After the three videos noted above were sent, the Sentai\_Sensei account user stated the following, which appeared to be directed to OCE: “Verification unsuccessful”. OCE then received a notification that he had been removed from the group.
- i. Below are excerpts from the communications in the #underfifteen group chat and the private messages that were exchanged with the Sentai\_Sensei and thebestone1985 account users:

Group Chat:

*Initial Standard Message:*

STOP

If you do not have a profile picture on your account, put one on BEFORE anything else. You will not be verified without one.

-----  
Welcome! Say hello to everybody and state your ASL within 2 minutes upon entry or you WILL be automatically removed.

TO VERIFY you will be asked to PM either TWO pictures or ONE video featuring "young" content to the active VERIFYING ADMIN. They will share your content with the rest of the group to confirm your verification.

Verifying Admins

GEO (@sentai\_sensei);  
Jasmine (@jazzybear2021);  
naughty (@thebestone1985);  
princess (@prinxessbubble5).

Content Moderators

GEO "THE BANHAMMER"  
Jasmine  
Mike Stevens  
ameli Holzer

GROUP RULES:

- 1) Share whatever you want, no age limits. However, NO hardcore rape, or any other material that could be considered violent, portray discomfort, pain, crying, or you will be banned from the group upon discovery. If you have questions about what you are allowed to share, please consult with an active admin
- 2) NO TRADING! Please share with the group. If you can't share yet ask an active admin to share for you
- 3) DO NOT post advertisements of any kind before you're verified or you will be banned
- 4) DO NOT invite users without consulting with an active admin
- 5) No links to other groups are allowed in main chat
- 6) DO NOT PM ANYONE without prior consent from the member you are trying to contact
- 7) Dont be mean, this chat isn't for fighting
- 8) KEEP ACTIVE! Oldest talkers have a risk of being removed

ADDITIONAL UPDATES:

- 1) If an admin is not currently available to verify, send your verifications to GEO "THE BANHAMMER" and he will get to them upon returning. If you fail to do so you will be removed no questions asked.
- 2) The following words are now forbidden to use in chat and will result in you being BANNED if said:  
TRADE, CRY, RAPE, ABUSE, TORTURE, or any racist language.  
This is a potentially incomplete list and is subject to change.

OCE:	Hello
OCE:	16 f Utah
Rebel1030:	Hey there
OCE:	Who do I PM?
thebesttone1985:	Pm me
Sentai_Sensei:	Hannah, can I have a word with you?
thebesttone1985:	And verify with me
Rebel1030:	Hannah?
Sentai_Sensei:	Activity
Unknown User:	<i>Posts information regarding other users' account activities</i>
Sentai_Sensei:	Are you still working that verification naughty?
thebesttone1985:	Yea
thebesttone1985:	<i>Sends video depicting possible child pornography</i>
thebesttone1985:	From rebel
thebesttone1985:	<i>Sends video depicting child pornography</i>
thebesttone1985:	<i>Sends video depicting child pornography</i>
thebesttone1985:	Also from rebel
Rebel1030:	Thank you
Sentai_Sensei:	Verification unsuccessful
OCE:	<i>Receives message stating: "You have been removed from the group"</i>

Private Messages with thebesttone1985 Account User:

OCE:	Hello
thebesttone1985:	Hi to verify I need 2 pics or 1 vid of young content plz
OCE:	Of me?
OCE:	<i>Sends image of a clothed female</i>
thebesttone1985:	No
thebesttone1985:	Read the sec part of the rules k
OCE:	Ok
thebesttone1985:	Hey pm geo plz u have 2 mins
OCE:	Ok

Private Messages with Sentai\_Sensei Account User:



OCE: Hey  
OCE: *Sends image of a clothed female*  
Sentai\_Sensei: Hello, I asked naughty to have you contact me because the way you entered the chat was actually violation of Rule #4, but it wasn't your fault. I saw that you were invited in by Hannah J. We don't typically allow people in to the group that were invited by other members, that's to help control the climate here. I'm trying to reach Hannah to discuss that with her so if you can just standby for a moment please?

OCE: Ok  
OCE: I have a 16 yo female  
Sentai\_Sensei: Ok, sorry about that. So verifications for this group are typically pictures or videos of young content, meaning cp. Do you understand what this group is for first off?

OCE: Yes other parents with yung kids to trade Original Content or live  
OCE: Mainly parents active in yung incest mmmmmm  
OCE: Is that fine?  
Sentai\_Sensei: So as far as verification content is concerned, we only accept things like young nudes or something close to it. They are also shared into the chat to validate the verification. Do you understand that?

OCE: Yes I do, but I want a fair trade of my 16 yo dau with someone else. If this isn't a parent group active with their yung ones I totally understand maybe it's not the right group for me. I'm just a horny perv dad lol

OCE: Just looking for like minded pervs  
Sentai\_Sensei: Ok, so the ASL that you posted in chat was false?  
OCE: No I have a 16 yo f in Utah. That's where I live and hoping that there is a local parent as well

Sentai\_Sensei: But your OWN asl is that of an older male, is that accurate?  
OCE: Yes sorry. I'm a 38 yo dad with a 16 yo dau  
OCE: Sorry for the confusion  
Sentai\_Sensei: Ok, so you are in the wrong kind of group. This is not a trading group at all to begin with, only a sharing group. So because you weren't truthful about the ASL in chat, I need to ask you to respectfully leave

OCE: No worries brother. Happy hunting. Let me know if you find a dad or mom out there having sex with their little ones.

Subpoenas Issued in 2022

59. On or around March 15, 2022, MediaLab.ai Inc. was served with an administrative subpoena requesting subscriber information for the Sentai\_Sensei Kik account as well as the log of IP addresses that were utilized to access the account. Records received from MediaLab.ai Inc. in response to the subpoena included the following information:

- a. The Sentai\_Sensei Kik account was created on or around September 12, 2021.
  - i. It was noted that the Kik account was created approximately 16 days after the search warrant was executed at the **SUBJECT PREMISES** on or around August 27, 2021.
- b. The current profile name for the account was "GEO". However, the profile name had been changed on several occasions.
- c. The email address of sentai.sensei@gmail.com was associated with the account. The records identified that this email address had not been confirmed or verified by a representative of MediaLab.ai Inc.
- d. The Kik account was utilized on a Samsung Android device bearing Model SM-S111DL on or around March 17, 2022.
  - i. It was noted that this make and model of an Android device matches the make and model of the cellular telephone that **GIBBS** brought with him to the FBI office when he was arrested on or around September 15, 2021. As noted above, this telephone was released to **GIBBS'** father.
- e. The user's birthday was listed as being XX/XX/1988 (redacted for purposes of this Affidavit).
  - i. This birthday matches **GIBBS'** date of birth.
- f. The log of IP addresses utilized to access the account was provided for the time period of September 12, 2021 through March 17, 2022. Review of the log provided the following information:
  - i. The account was accessed on a total of approximately 13,024 occasions as follows:
    1. On approximately 36 occasions during the approximate time period of September 12, 2021 through September 13, 2021;
    2. On approximately one occasion on or around September 29, 2021

(approximately five days after **GIBBS** was released on bond following his arrest for the child pornography charges); and

3. On approximately 12,987 occasions during the approximate time period of January 27, 2021 through March 17, 2021 (on a daily basis, multiple times per day, for the entire time period).
  - ii. The IP address of 99.88.157.4 was utilized to access the account on approximately 7,033 occasions.
    1. This is the same IP address that was utilized in 2021 to access the karate\_niidan06@yahoo.com account, and which was subscribed to “GEORGE GIBBS” at the **SUBJECT PREMISES** (as detailed above).
    2. This was the only IP address that was utilized to access the account on or around March 12, 2022 (the date that OCE participated in the #underfifteen group chat and communicated directly with the Sentai\_Sensei Kik account user).
    3. This IP address was utilized to access the account as recently as on or around March 14, 2022.
  - iii. A number of IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately 5,540 occasions.
  - iv. A number of IP addresses that appear to be associated with VPN’s were utilized to access the account on approximately 451 occasions.
60. On or around March 23, 2022, AT&T was served with an administrative subpoena requesting subscriber information for the IP address of 99.88.157.4 on March 12, 2022, on one of the times that it was utilized to access the Sentai\_Sensei Kik account. Records received from AT&T in response to the subpoena identified that the IP address was subscribed to “GEORGE GIBBS” at the **SUBJECT PREMISES**.
61. Also on or around March 23, 2022, Google LLC was served with an administrative subpoena requesting subscriber information for the sentai.sensci@gmail.com Google account, as well as the log of IP addresses utilized to access the account. Records received from Google LLC in response to the subpoena provided the following information:
- a. The account was created on or around September 5, 2021.
    - i. It was noted that the account was created approximately nine days after the search warrant was executed at the **SUBJECT PREMISES** on or around

August 27, 2021, and approximately seven days before the Sentai\_Sensei Kik account was created.

- b. The user name for the account was “**GEORGE GIBBS**”.
  - c. The telephone number associated with the account was 937-271-3364.
  - d. The log of IP addresses utilized to access the account was provided for the time period of January 27, 2022 through March 7, 2022. Review of the log provided the following information:
    - i. The account was accessed on a total of approximately eight occasions.
    - ii. The IP address of 99.88.157.4 (the IP address subscribed to “**GEORGE GIBBS**” at the **SUBJECT PREMISES**) was utilized to access the account on approximately one occasion.
    - iii. Dynamic IP addresses serviced by AT&T were utilized to access the account on approximately four occasions.
    - iv. IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately three occasions.
62. On or around March 24, 2022, Verizon was served with an administrative subpoena requesting records of all telephone numbers that connected to a sample of three of the IP addresses that had been utilized to access the Sentai\_Sensei Kik account on the dates and times that those IP addresses had accessed the account. Records received from Verizon in response to the subpoena identified that telephone number 937-271-3364 (the telephone number associated with the sentai.sensei@gmail.com Google account) had connected to all three of the IP addresses on the dates and times listed in the subpoena.
63. On or around April 20, 2022, Verizon was served with an administrative subpoena requesting subscriber information for telephone number 937-271-3364 (the telephone number associated with the sentai.sensei@gmail.com Google account). Records received from Verizon in response to the subpoena provided the following information:
- a. The telephone had been sold by TracFone (a reseller of cellular telephones), and no subscriber information was maintained for the account.
  - b. The telephone number was activated on or around September 3, 2021 (approximately seven days after the execution of the search warrant at the **SUBJECT PREMISES**). The account was presently active.
  - c. The device utilizing the cellular telephone number was a Samsung Model SM-

S111DL telephone bearing an IMEI number of 352319150023008.

- i. The make and model of the cellular telephone matches the Android device that was used to access the Sentai\_Sensei Kik account on or around March 17, 2022.
- ii. The make, model, and IMEI of the cellular telephone matches the device that **GIBBS** brought with him to the FBI office when he was arrested on or around September 15, 2021.

#### Review of Social Media Accounts

64. On or around April 15, 2022, an FBI investigator searched publicly available information on various social media websites and messenger applications for any possible accounts associated with the email address sentai.sensei@gmail.com and the telephone number 937-271-3364. The analyst located a WhatsApp account (an encrypted messenger application) associated with telephone number 937-271-3364.
  - a. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize encrypted messenger applications such as WhatsApp to trade child pornography files.
65. Also on or around April 15, 2022, an FBI investigator searched various social applications for other social media accounts with a user name of Sentai\_Sensei. An Instagram social media account with an account name of Sentai\_Sensei was located. The publicly available account information identified that the profile name for the account was "**GEORGE GIBBS III**". The profile picture for the account was an image depicting **GIBBS** holding his son.

#### Conclusion Regarding New Accounts

66. Based on all of the information detailed in the Affidavit, there is probable cause to believe that **GIBBS** is the user of the following:
  - a. The Sentai\_Sensei Kik account;
  - b. The sentai.sensei@gmail.com Google account; and
  - c. The Samsung Model SM-S111DL cellular telephone bearing telephone number 937-271-3364.
67. There is also probable cause to believe the following:



- a. **GIBBS** has utilized his Samsung cellular telephone and the Sentai\_Sensei Kik account to distribute and receive child pornography files.
- b. **GIBBS** has administered the #underfifteen Kik group. Within this group, **GIBBS** has conspired with others to distribute and receive child pornography files.

Evidence Sought in Search Warrants

68. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.
69. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
70. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
71. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).
72. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
73. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the

production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.

74. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
75. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.
76. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.
77. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.
78. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

79. As described above and in Attachments B-1 and B-2, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES** and on the person of

**GIBBS**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

80. *Probable cause.* I submit that if a computer or storage medium is found on the **SUBJECT PREMISES** and on the person of **GIBBS**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:
  - a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
  - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
  - c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
  - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
81. *Forensic evidence.* As further described in Attachments B-1 and B-2, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** and on the person of **GIBBS** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer

user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
  - d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
  - e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
82. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of

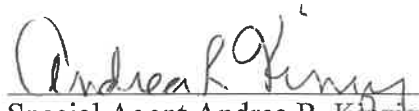


information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
  - c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
83. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**CONCLUSION**

84. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located at the **SUBJECT PREMISES**, on the person of **GIBBS**, and on the Computer and Electronic Media (as defined in Attachments B-1 and B-2) located at the **SUBJECT PREMISES** and on the person of **GIBBS**: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1).
85. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN  
Before me this 22nd of April 2022

  
HONORABLE MICHAEL J. NEWMAN  
UNITED STATES DISTRICT COURT JUDGE

